ALLIANT 2 GWAC UNRESTRICTED MASTER CONTRACT

CONFORMED CONTRACT
June 2019

SECTION C - CONTRACT SCOPE OF WORK AND PERFORMANCE WORK STATEMENT

C.1 SCOPE OF WORK OBJECTIVE

The Alliant 2 GWAC will provide Federal Government agencies with integrated Information Technology (IT) solutions for evolving needs on a global basis. This Master Contract allows for the application of technology to meet business needs including the ability to perform all current, leading edge and/or emerging IT services required to satisfy all IT services requirements anywhere and anytime worldwide.

Integrated IT solutions are comprised of IT components described below in Section C.4, and may be tailored in Task Order Requests to meet agencies' mission needs. Work may be performed at Government and Contractor facilities located throughout the world, as specified in each Task Order, to provide a variety of IT solutions and support services. IT services and solutions within scope of this Master Contract include new, leading edge and emerging technologies that will evolve over the life of the Master Contract as supported by the Federal Enterprise Architecture (FEA), Department of Defense Information Enterprise Architecture (DoD IEA) Reference Models, and the associated reference models.

C.2 SCOPE OF WORK OVERVIEW

The Master Contract provides maximum flexibility in acquiring an IT services-based solution for any conceivable IT services-based requirement driving government savings through efficiencies and improved reporting data with greater integrity while maintaining an "Anything IT Anywhere" philosophy.

The Master Contract scope includes any and all components of an integrated IT services-based solution, including all current leading edge technologies and any new technologies, which may emerge during the Master Contract period of performance. **All IT development methodologies, including Agile which is an encouraged methodology, are supported**. The Master Contract scope also includes IT services-based support of National Security Systems, as defined in FAR 39.002. The Master Contract provides IT solutions through performance of a broad range of services, which may include the integration of various technologies critical to the services being acquired. The foundation of the Scope of Master Contract is built on the most current FEA and DoD IEA Reference Models. (See links under Resources Section C.10). As the definition of IT changes over the lifecycle of the Master Contract with the evolving FEA and DoD IEA models, the scope of the Master Contract will be considered to coincide with the current IT definition at any given time.

By nature of the alignment to FEA and DoD IEA, the Master Contract includes any and all emerging IT components, IT services, and ancillary elements as they arise as required to successfully achieve the agency's mission. Therefore, because technological advances

over the term of this Master Contract are inevitable, the scope of this Master Contract takes into consideration that Task Order Requirements are permitted to include any future IT services with their integral and necessary ancillary IT components and services as they arise during the entire term of this contract. The scope of the Master Contract includes every conceivable aspect of **IT Services**, including **but not limited to:**

- 3-D Printing Integration
- Agile Development
- Big Data
- Biometrics /Identity Management
- Cloud Computing
- Context-aware Computing
- Critical Infrastructure Protection and Information Assurance
- Cyber Security
- Data-Centers and Data-Center Consolidation
- Digital Government
- Digital Trust and Identity Integration and Management
- Digitization and Imaging
- Energy and Sustainability Measurement and Management
- Enterprise App Stores and Mobile Security
- Enterprise Resource Planning
- Integration Services
- Internet of Things
- IPV6 migration & upgrades
- IT Helpdesk
- IT Operations and Maintenance
- IT Services for Healthcare
- IT Services for Integrated Total Workplace Environment
- Mobile-Centric Application Development, Operations and Management
- Modeling and Simulation
- Network Operations, Infrastructure, and Service Oriented Architecture
- Open Source Integration and Customization
- Outsourcing IT Services
- Sensors, Devices and Radio Frequency Identification (RFID)
- Shared IT Services
- Software Development
- Virtualization
- Voice and Voice Over Internet Protocol (VOIP)
- Web Analytics
- Web Application & Maintenance
- Web Services
- Web Hosting

C.3 FOUNDATION OF THE SCOPE OF WORK

Overview of Federal Enterprise Architecture Framework (FEAF) and Department of Defense Information Enterprise Architecture (DOD IEA)

(1) Solutions to Integrated IT requirements are comprised of some or all components and functional areas associated with FEA and DoD IEA and may be tailored to meet agency needs. By aligning the scope of the Master Contract to FEA/DoD IEA users have access to the entire spectrum of current and emerging IT service, all ancillary services, products and personnel required to successfully meet the agency mission.

(2) The Contractor shall promote IT solutions that support Federal government operational requirements for standardized technology and application service components. This shall facilitate integration requirements for broad Federal IT and e-Gov Initiatives, as well as promote the sharing, consolidation, and "re-use" of business processes and systems across the Federal government. The Contractor shall promote the use of open source solutions and open technology development where practicable to enable this "re-use" in accordance with the underlying tenets of FEA/DoD IEA and to address any number of areas of interest within the limits of IT and supporting services and disciplines.

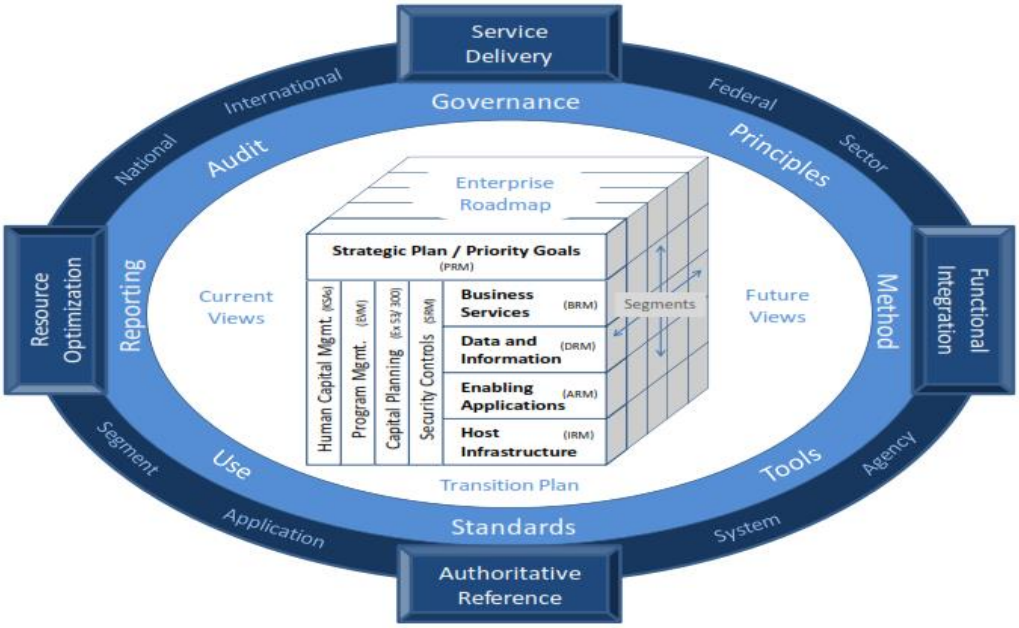


Figure 1 - Federal Enterprise Architecture

The Master Contract leverages the existing FEA and the DoD IEA version 2.0 as the basis of its IT scope.

FEA & DOD IEA represent a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy. Enterprise architecture applies architecture principles and practices to guide organizations through the business, information, process, and technology changes necessary to execute their strategies. This includes everything from a small mobile application development project to the design, installation and migration to a complex network serving hundreds of thousands of users. These practices utilize the various aspects of an enterprise to identify, motivate, and achieve these changes.

Each reference model represents and includes a number of functional areas required to meet an objective.

C.3.1 FEA Reference Model Detailed Descriptions

Enterprise Architecture (EA) supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail. The Common Approach to Federal Enterprise Architecture, released in May 2012 as part of the federal CIO's policy guidance and management tools for increasing shared approaches to IT service delivery, presents an overall approach to developing and using Enterprise Architecture in the Federal Government. The Common Approach promotes increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. This includes principles for using EA to help agencies eliminate waste and duplication, increase-shared services, close performance gaps, and promote engagement among government, industry, and citizens.

The Federal Enterprise Architecture Framework v2 describes a suite of tools to help government planners implement the Common Approach. At its core is the Consolidated Reference Model (CRM), which equips OMB and Federal agencies with a common language and framework to describe and analyze investments. It consists of a set of interrelated "reference models" that describe the six sub architecture domains in the framework:

- Strategy
- Business
- Data
- Applications
- Infrastructure
- Security

These are designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. Also, by applying all six reference models, agencies can establish a line of sight from the strategic goals at the highest organizational level to the software and hardware infrastructure that enable achievement of those goals. Collectively, the reference models

comprise a framework for describing important elements of federal agency operations in a common and consistent way.

To apply the framework to an agency's specific environment, the agency should develop a set of "core" artifacts to document its environment within the framework presented by the CRM. Each subarchitecture domain represents a specific area of the overall framework and has particular artifacts, based on EA best practices, which are described and recommended in the Framework and Artifacts document. The type and depth of documentation actually used by the agency should be guided by the need or detail and answers to questions about requirements, applicable standards, timeframes, and available resources.

The real value to the agency of developing an Enterprise Architecture is to facilitate planning for the future in a way that transforms the government while making it more efficient. The agency can use the EA process to describe the enterprise as it currently is and determine what the enterprise should look like in the future, so that it can make plans to transition from the current state to the future state. The Collaborative Planning Methodology provides steps for planners to use throughout the planning process to flesh out a transition strategy that will enable the future state to become reality. It is a simple, repeatable process that consists of integrated, multi-disciplinary analysis that involves sponsors, stakeholders, planners, and implementers.

The agency will create an Enterprise Roadmap to document the current and future architecture states at a high level and presents the transition plan for how the agency will move from the present to the future in an efficient, effective manner. The agency's Enterprise Roadmap combines the artifacts developed for the EA, both current and future state versions, with a plan developed through the Collaborative Planning Methodology. This creates awareness, visibility and transparency within an organization to facilitate cross-organization planning and collaboration. It maps strategy to projects and budget and helps identify gaps between investment and execution, as well as dependencies and risks between projects.

All in all, the Federal Enterprise Architecture Framework v2 helps to accelerate agency business transformation and new technology enablement by providing standardization, analysis and reporting tools, an enterprise roadmap, and a repeatable architecture project method that is more agile and useful and will produce more authoritative information for intra- and inter-agency planning, decision making, and management.

Overview of the Collaborative Planning Methodology (CPM)

Planning is done to affect change in support of an organization's Strategic Plan, and the many types of planners (e.g., architects, organization and program managers, strategic planners, capital planners, and other planners) must work together to develop an integrated, actionable plan to implement that change. Planning should be used to determine the exact changes that are needed to implement an organization's Strategic Plan, enable consistent decision-making, and provide measurable benefits to the

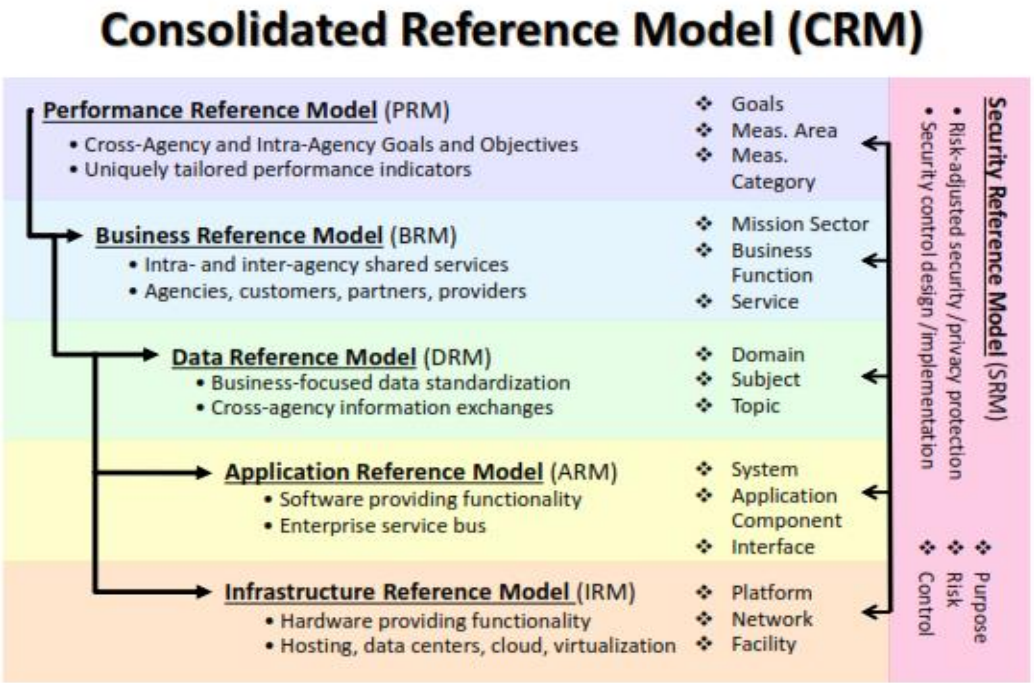
organization. In short, an organization's Strategic Plan should be executed by well-rounded planning that results in purposeful projects with measurable benefits.

In today's environment, which demands more efficient government through the reuse of solutions and services, organizations need actionable, consistent, and rigorous plans to implement Strategic Plans and solve priority needs. These integrated plans should support efforts to leverage other Federal, state, local, tribal, and international experiences and results as a means of reusing rather than inventing from scratch. Plans should be consistent and rigorous descriptions of the structure of the organization or enterprise, how IT resources will be efficiently used, and how the use of assets such as IT will ultimately achieve stated strategies and needs.

Consolidated Reference Models

The Consolidated Reference Model of the FEA equips OMB and Federal agencies with a common language and framework to describe and analyze investments. It consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. Collectively, the reference models comprise a framework for describing important elements of federal agency operations in a common and consistent way. Through the use of the FEAF and its vocabulary, IT portfolios can be better managed and leveraged across the federal government, enhancing collaboration and ultimately transforming the Federal government.

The five reference models in version 1 the FEA have been regrouped and expanded into six in the current version of the FEA.



With edits for brevity, the following reference model **summarized** descriptions were taken from *OMB's FEA Consolidated Reference Model Document Version 2. dated January 29, 2013*.

Significantly more detail about the structure, taxonomy, and associated methods of the reference models is available online:

See Attachment J-8 Website References.

The motivating purpose of adopting The FEA as scope guidance is to help establish business driver alignment with any number of the reference models which support all possible underlying technologies required to meet an agency objective as well as offering the baseline for the technical vocabulary required in any given task.

Performance Reference Model (PRM)

The PRM is designed to provide linkage between investments or activities and the strategic vision established by agencies and the Federal government. Historically, linking information management investments and activities has been anecdotal due to a lack of standard approach to describing Agency and cross agency performance attributes. The GPRA Modernization Act of 2010 requires the government to publish performance information through a central web site and make strategic plans and performance reports available in machine readable formats. This advance enables more comprehensive and consistent linking of investments and activities to Agency strategic goals and objectives, Agency priority Goals, Cross Agency Priority goals and management areas of focus. The PRM leverages the requirements of the GPRA Modernization Act to establish mechanisms to link directly to the authoritative performance elements published in compliance with the law and provides the means for use of future developments in the mandated central performance website Performance.gov.

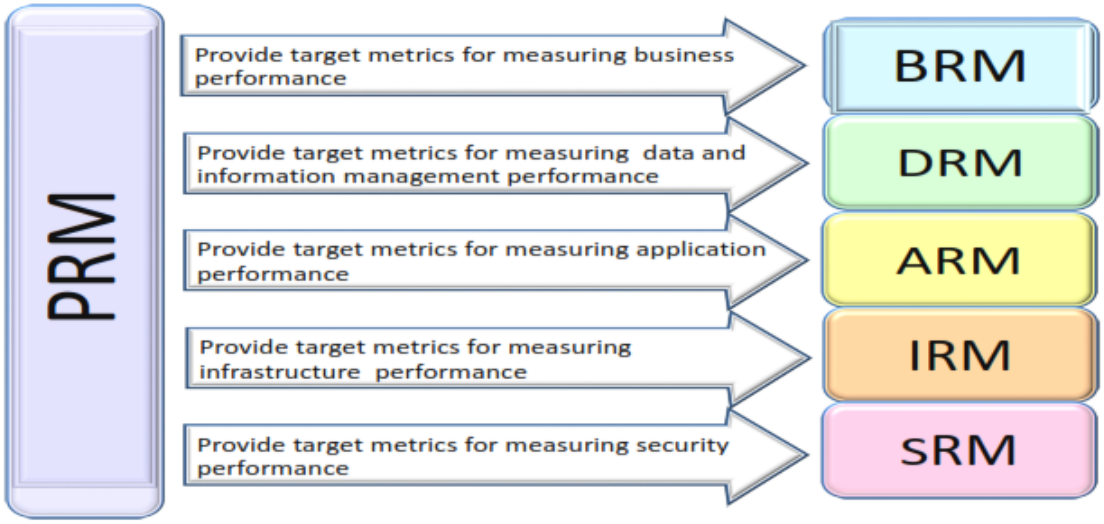
There are three areas to the Performance Reference Model. The first is the Goal. This enables grouping of investments and activities through a common and authoritative framework established by agencies in compliance with OMB direction and the GPRA Modernization Act. It allows the identification of common performance elements across investments or activities, and in the future, will enable cross platform information linkages between systems such as Performance.gov and the IT Dashboard.

This linkage provides the logical relationships necessary to consistently provide much richer insights into details of the supported performance areas than previously feasible.

The second area of the Performance Reference Model is Measurement Area. This describes the manner in which the investment or activity supports the achievement of the supported performance element identified by the Agency Goal. Measurement Areas apply to the more detailed performance indicators associated with the investment of activity rather than the functions of the investment or activity. Investment or activity performance indicators should have a clear linkage to the activities, of course, but it is important to recognize that investments or activities may align to multiple measurement areas.

The third area, Measurement Category, refines Measurement Area. Any Measurement Category may be applied to any Goal.

The PRM, like all other reference models, is intended to work in concert with other reference models. The combined descriptive qualities of the multiple perspectives afforded by assigning different reference model perspectives to investments or activities can provide rich insights into what, why and how the investments or activities are undertaken. Previous versions of the PRM included mission function characteristics that were redundant to the BRM. In this version of the PRM the Measurement Category codes have been streamlined to better identify the means by which performance is achieved. Including BRM and PRM mappings with an investment or activity provides information about the strategic basis (why) through the Agency Goal, the means (how) through the measurement category, and the mission functions involved (what) through the BRM taxonomy. Additional mappings to other reference models provide further context for the investment or activity with the SRM providing information about risk, the DRM about the information involved and the ARM and IRM providing the technical details about the implementation.



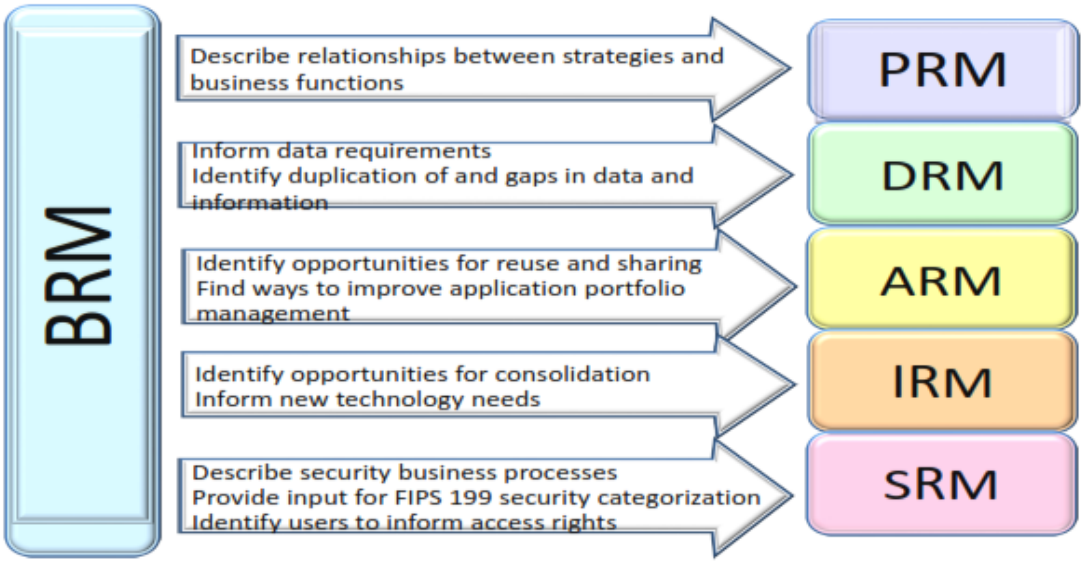
Business Reference Model (BRM)

The BRM is a classification taxonomy used to describe the type of business functions and services that are performed in the Federal Government. By describing the Federal Government using standard business functions rather than an organizational view, the BRM promotes cross-government collaboration. It enables business and IT leaders to discover opportunities for cost savings and new business capabilities that help to achieve strategic objectives. The BRM describes the "What we do" of the Federal enterprise through the definition of outcome-oriented and measurable functions and services.

While the BRM provides a standardized way of classifying government functions, it is only a model; its true utility and value is realized when it is applied and effectively used

in business analysis, design and decision support that help to improve the performance of an agency, bureau or program.

BRM is informed by the PRM and informs the other reference models. At the high level, the BRM relationship and tie-in to the other reference models is illustrated in the following table:



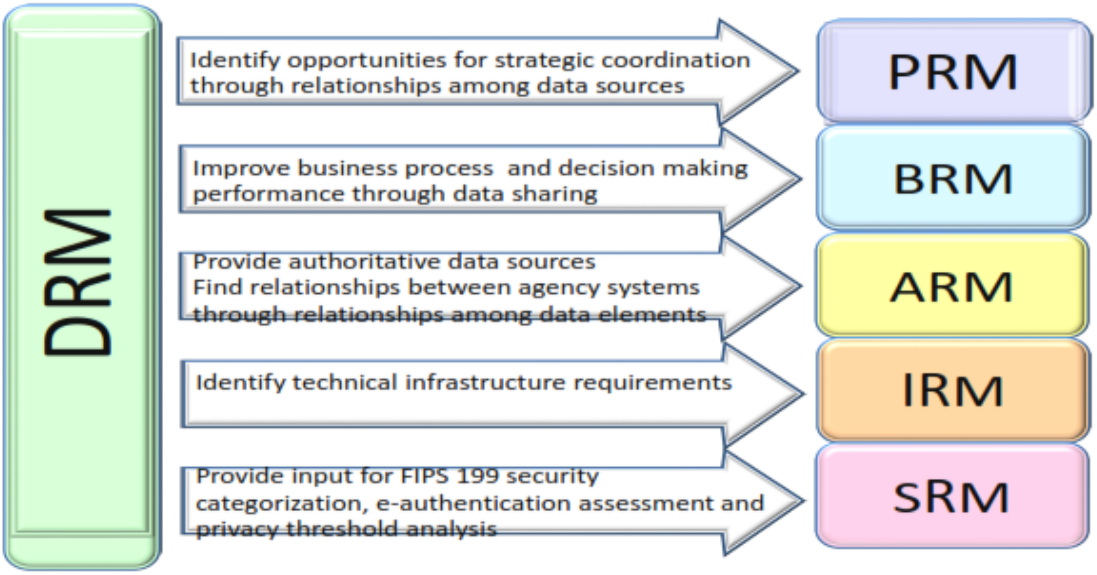
The BRM forms a key part in delivering expected outcomes and business value to an organization. By using a standard taxonomy to classify functions, investments, programs, services and other elements across the Federal Government, the BRM is useful in identifying opportunities for cost reduction, collaboration, shared services, and solution reuse in agency IT portfolios and intra- and inter-agency collaboration.

Data Reference Model (DRM)

The DRM's primary purpose is to promote the common identification, use, and appropriate sharing of data/information across the federal government. The DRM is a flexible and standards-based framework to enable information sharing and reuse via the standard description and discovery of common data and the promotion of uniform data management practices. The DRM provides a standard means by which data may be described, categorized, and shared, and it facilitates discovery and exchange of core information across organizational boundaries.

As a reference model, the DRM is presented as an abstract framework from which concrete implementations may be derived. The DRM's abstract nature will enable agencies to use multiple implementation approaches, methodologies and technologies while remaining consistent with the foundational principles of the DRM.

The DRM is closely linked with the other five reference models of the Consolidated Reference Model Framework. At the high level, the DRM relationship and tie-in to the other reference models is illustrated in the following table:



The DRM provides guidance for agencies to leverage existing Data Assets across the government. The DRM increases the Federal government's agility in drawing out the value of information as a strategic asset. This reference-able, conceptual approach facilitates information sharing and reuse across the Federal government.

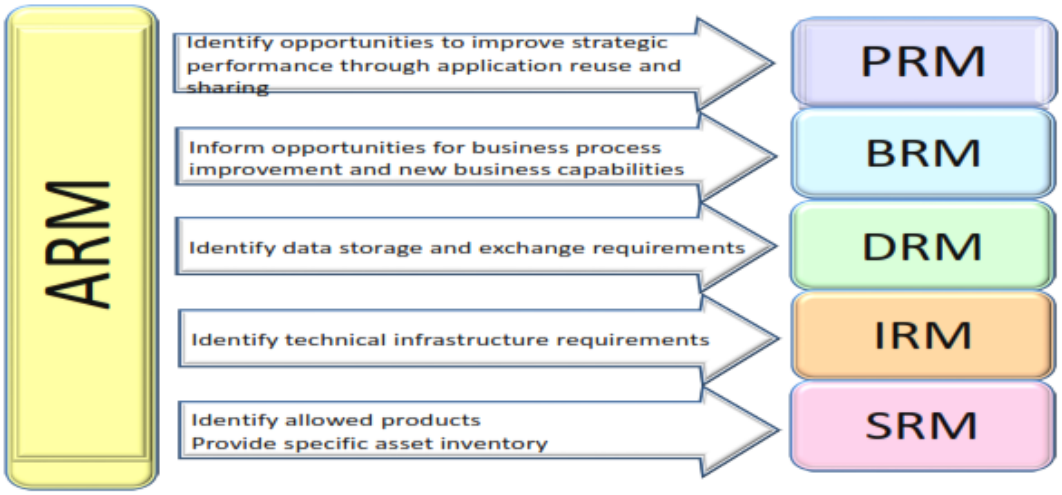
Application Reference Model (ARM)

The purpose of the ARM is to provide the basis for categorizing applications and their components. As agencies map their current and planned Information Systems to the ARM categories, gaps and redundancies will become evident, which will aid in identifying opportunities for sharing, reuse, and consolidation or renegotiation of licenses. This information may be used in conjunction with the other Reference Models to identify these opportunities.

For the purposes of the CRM, Application is defined as: Software components (including websites, databases, email, and other supporting software) resting on Infrastructure that, when aggregated and managed, may be used to create, use, share, and store data and information to enable support of a business function.

The ARM is a categorization of different types of software, components and interfaces. It categorizes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (e.g. firmware) because these are contained in the IRM. It also does not contain mission-specific categorizations for systems because that information can be obtained from mappings to the BRM.

The ARM is closely linked with the other five reference models of the Consolidated Reference Model Framework. At the high level, the ARM relationship and tie-in to the other reference models is illustrated in the following table:



Infrastructure Reference Model (IRM)

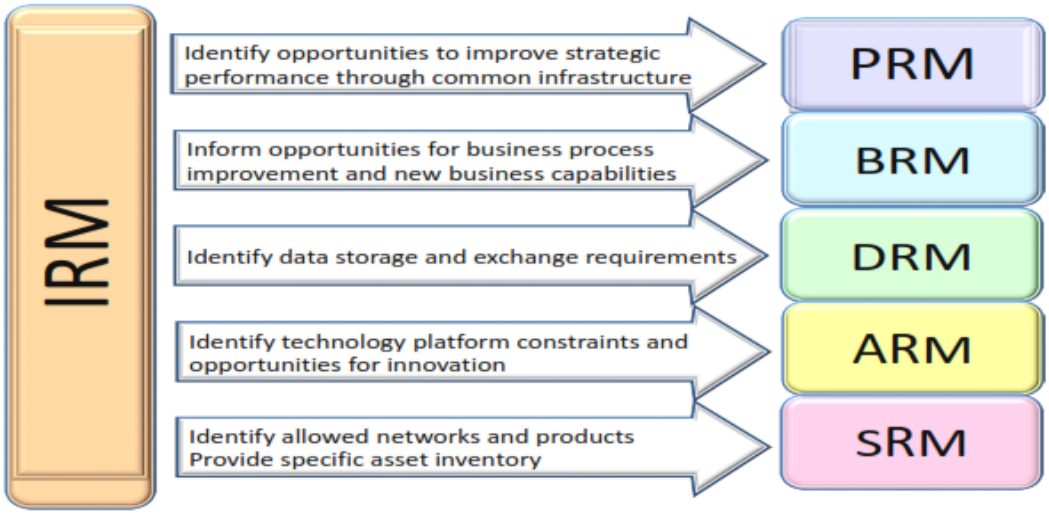
The IRM is the taxonomy based reference model for categorizing IT infrastructure and the facilities and network that host the IT infrastructure. The IRM supports definition of infrastructure technology items and best practice guidance to promote positive outcomes across technology implementations.

For the purposes of the CRM, Infrastructure is defined as: The generic (underlying) platform consisting of hardware, software and delivery platform upon which specific/customized capabilities (solutions, applications) may be deployed.

The IRM implementation enables sharing and reuse of infrastructure to reduce costs, increase interoperability across the government and its partners, support efficient acquisition and deployment, and enable greater access to information across enterprises.

In addition to providing a categorization schema for IT infrastructure assets, the IRM enables analysis of IT infrastructure assets at a Department or Agency level as well as at a Federal Government level. In the Federal context, the IRM is adopted and used to conduct Government-wide analysis of IT infrastructure assets and to identify consolidation initiatives. In the Department or Agency context, the IRM is used to drive good IT infrastructure asset management practices such as identifying end-of-life assets before they affect the mission of an organization and to identify opportunities for sharing and consolidating infrastructure.

The IRM is closely linked with the other five reference models of the Consolidated Reference Model Framework (CRM). At the high level, the IRM relationship and tie-in to the other reference models is illustrated in the following table:



Security Reference Model (SRM)

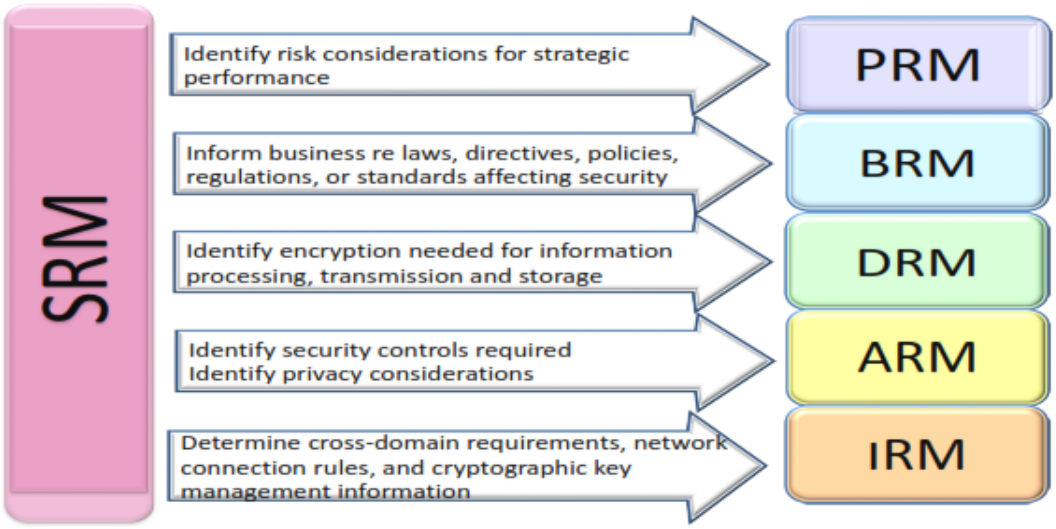
Security is integral to all architectural domains and at all levels of an organization. As a result, the SRM must be woven into all of the sub-architectures of the overarching EA across all the other reference models and it must be considered up and down the different levels of the Enterprise. Enterprise Architecture Governance is the perfect place for security standards, policies, and norms to be developed and followed, since it is an enforcement point for Information Technology investments.

The SRM allows architects to classify or categorize security architecture at all scope levels of the Federal Architecture: International, National, Federal, Sector, Agency, Segment, System and Application. At the highest levels, the SRM is used to transform federal laws, regulations, and publications into specific policies. At the segment level, the SRM is used to transform department specific policies into security controls and measurements. At the system level, it is used to transform segment controls into system specific designs or requirements. Each level of the SRM is critical to the overall security posture and health of an organization and/or system.

The SRM helps business owners with risk-based decision-making to achieve security objectives by understanding the purpose and impact of security controls on business processes or IT systems.

Security integration across layers of the architecture is essential to ensure the protection of information and IT assets. Security must start at the business layer and work its way down to the application and infrastructure layers.

At the high level, the SRM relationship and tie-in to the other reference models is illustrated below:



Linking security and privacy to agency enterprise architecture, including agency performance objectives, business processes, data flows, applications and infrastructure technologies, ensures that each aspect of the business receives appropriate security and privacy considerations. Additionally, addressing security and privacy through enterprise architecture promotes interoperability and aids in the standardization and consolidation of security and privacy capabilities.

C.4 COMPONENTS OF AN IT SOLUTION

The Contractor shall provide Infrastructure and related services, Applications and related services, and IT Management Services to support agencies' integrated IT solution requirements.

In order to provide a common framework for defining and understanding the components of an IT solution, this section will refer to terminology included in the FEA and DoD IEA. Usage of this terminology or structure is not required within individual Orders placed on this contract.

The Contractor shall promote IT solutions that support Federal government operational requirements for standardized technology and application service components. This shall facilitate integration requirements for broad Federal IT and e-Gov initiatives, as well as promote the sharing, consolidation, and "re-use" of business processes and systems across the Federal government. The Contractor shall promote the use of open source solutions and open technology development where practicable to enable this re-use.

Within each section below, an overview of the contract solution and service offerings is provided, followed by work to be performed relative to Order requirements. Components of an IT solution indicated in this Scope are not meant to be all-inclusive, but rather general indications of the types of services and goods within a given category. Other

services and goods not listed, which adhere to the definition for each section are also within scope.

C.4.1 Infrastructure

Infrastructure includes hardware, software, licensing, technical support, and warranty services from third party sources, as well as technological refreshment and enhancements for that hardware and software.

This section is aligned with the FEA/DoD IEA, which describes these components using a vocabulary that is common throughout the entire Federal government. Infrastructure includes complete life cycle support for all hardware, software, and services represented above, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition of these components. The services also include administration and help desk functions necessary to support the IT infrastructure. Infrastructure serves as the foundation and building blocks of an integrated IT solution. It is the hardware, which supports Application Services and IT Management Services; the software and services which enable that hardware to function; and the hardware, software, and services which allow for secure communication and interoperability between all business and application service components.

Infrastructure services facilitate the development and maintenance of critical IT infrastructures required to support Federal government business operations. This section includes the technical framework components that make up integrated IT solutions. One or any combination of these components may be used to deliver IT solutions intended to perform a wide array of functions which allow agencies to deliver services to their customers (or users), whether internal or external, in an efficient and effective manner.

C.4.1.1 Service Access and Delivery

These components are responsible for facilitating the end-to-end collection and distribution of data that is either entered or requested by a user. These components include all functions necessary to communicate in a client-server environment. Examples of these components include, but are not limited to:

- Web browsers
- Virtual Private Network (VPN)
- Remote Authentication Dial-In User Service (RADIUS)
- Peer-to-peer
- Section 508 compliance
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)

C.4.1.2 Service Platform and Infrastructure

These components include all functions necessary for processing and storing data. These components provide and manage the resources available for Application Services. Examples of these components include, but are not limited to:

- Desktops, laptops, servers, mainframes, routers, switches, and printers.
- Asynchronous Transfer Mode (ATM) and T1
- Digital Subscriber Line (DSL), Ethernet, Windows/UNIX, Java/.NET
- Web server/portal
- Database, data storage, data warehouse
- Software development tools
- Testing, modeling, versioning, and configuration management.

C.4.1.3 Component Framework

These components consist of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. These components define higher level logical functions to provide services in a way that is useful and meaningful to users and other Application Services. Examples of these components include, but are not limited to:

- Digital certificates, biometrics;
- Business logic: JavaScript, Visual Basic
- Data interchange
- Simple Object Access Protocol (SOAP)
- Resource Description Framework (RDF)
- Data management
- Structured Query Language (SQL), Open DataBase Connectivity (ODBC), and Online Analytical Processing (OLAP).

C.4.1.4 Service Interface and Integration

These components define the discovery, interaction and communication technologies joining disparate systems and information providers. Application Services leverage and incorporate these components to provide interoperability and scalability. Examples of these components include, but are not limited to:

- Messaging-Oriented Middleware (MOM)
- Object Request Broker (ORB)
- Enterprise Application Integration (EAI)
- Extensible Markup Language (XML)
- Electronic Data Interchange (EDI)
- Web Services Description Language (WSDL)
- Universal Description, Discovery and Integration (UDDI)

C.4.2 Application Services

Application Services provide support for all applications and collaborative service capabilities. These services include support for developing and implementing enterprise and departmental-level applications. These applications may be "cross-cutting" in nature, with inter-related service processing components extending across/beyond the enterprise, or unique to a particular agency/department's mission requirements.

The Contractor shall promote, to the maximum extent practicable use of commercially available technologies (e.g. Commercial Off-the-Shelf (COTS) and non-developmental items) to support Federal government agencies' IT solution requirements. The Contractor shall provide competencies to employ agencies' enterprise architectures (EAs) as required by individual Orders, to support IT solutions development and implementation and alignment with the FEA.

Application Services include complete life cycle support, including planning, analysis, research and development, design, development, integration and testing, implementation, operations and maintenance, information assurance, and final disposition.

The Contractor shall provide Applications Services for systems required to support unique agency and departmental-level mission requirements, as specified in individual Orders. These services include support for existing and/or new/emerging mission requirements.

The following represents either components of applications or capabilities, which Application Services will support. Each particular area includes, but is not limited to, support for the described functions.

C.4.2.1 Customer Services

Customer Relationship Management (CRM): All aspects of the CRM process, including planning, scheduling, and control activities involved with service delivery. The service components facilitate agencies' requirements for managing and coordinating customer interactions across multiple communication channels and business lines.

Customer Preferences: Customizing customer preferences relative to interface requirements and information delivery mechanisms (e.g., personalization, subscriptions, alerts and notifications).

Customer Initiated Services: Initiating service requests and seeking assistance from government agencies via online communication channels (e.g., online help, tutorials, self-service, reservation/registration, multilingual support, scheduling).

C.4.2.2 Process Automation

Tracking and Workflow: Automated routing, tracking, and management of documents (e.g., process tracking, case management, and conflict resolution).

Routing and Scheduling: Automated distribution and scheduling activities (e.g., inbound/outbound correspondence management).

C.4.2.3 Business Management

Process Management: Development and implementation of standard methodologies and automated process management systems, to facilitate agencies' requirements for managing and monitoring activities surrounding their core business operations (e.g., change management, configuration management, requirements management, program/project management, governance/policy management, quality management, risk management).

Organizational Management: Collaboration and communication activities (e.g., workgroup/groupware, network management).

Investment Management: Selecting, managing, and evaluating agencies' investments and capital asset portfolios (e.g., strategic planning/management, portfolio management, performance management).

Supply Chain Management: All aspects of supply chain management, from the initial sourcing phase through customer delivery (e.g., procurement, sourcing management, inventory management, catalog management, ordering/purchasing, invoice tracking, storefront/shopping cart, warehouse management, returns management, logistics/transportation).

C.4.2.4 Digital Asset Services

Content Management: Content development, maintenance, updates, and distribution (e.g., content authoring, content review/approval, tagging/aggregation, content publishing/delivery, syndication management).

Document Management: Capturing, indexing, and maintaining documents (e.g., document imaging, optical character recognition (OCR), document revisions, library/storage, review/approval, document conversion, indexing/classification).

Knowledge Management: Collecting and processing data from multiple sources and generating information to support business requirements (e.g., information retrieval, information mapping/taxonomy, information sharing, categorization, knowledge engineering, knowledge capture/distribution/delivery, and smart documents).

Records Management: Administration of official government records (record linking/association, record storage/archival, document classification, document retirement, digital rights management).

C.4.2.5 Business Analytical Services

Analysis and Statistics: Applying analysis and statistics to examine/resolve business issues (e.g., mathematical, structural/thermal, radiological, forensics).

Visualization: Transforming data into graphical or image form (e.g., graphing/charting, imagery, multimedia, mapping/geospatial/elevation/global positioning systems (GPS), computer-aided design (CAD)).

Knowledge Discovery: Identifying and extracting information from multiple data source containing files stored in various formats (e.g., data mining, modeling, simulation).

Business Intelligence: Collecting information relevant to historical, existing, or future business needs (e.g., demand forecasting/management, balanced scorecard, decision support planning).

Reporting: Generating reports derived from single or multiple data sources (e.g., ad hoc reporting, standardized/canned reporting, OLAP).

C.4.2.6 Back Office Services

Data Management: Creating, using, processing, and managing data resources (e.g., data exchange, data mart, data warehouse, metadata management, data cleansing, extraction and transformation, data recovery).

Human Resources: Recruitment, training, and management of government personnel (e.g., recruiting, career development/retention, time reporting, awards/benefit management, retirement management, education/training, travel management).

Financial Management: Government financing and accounting activities (e.g., billing and accounting, credit/charge, expense management, payroll, payment/settlement, debt collection, revenue management, internal controls, auditing, activity based management, currency translation).

Asset/Material Management: Acquisition and management of Federal government assets (property/asset management, asset cataloging/identification, asset transfer/allocation/maintenance, facilities management, computers/automation management).

Development and Integration: Development and integration of systems across diverse operating platforms (e.g., legacy integration, enterprise application integration, data integration, instrumentation/testing, software development).

Human Capital/Workforce Management Development and Integration: Planning and supervisory operations surrounding government personnel (e.g., resource planning/allocation, skills management, workforce directory/locator, team/organization management, contingent workforce management).

C.4.2.7 Support Services

Security Management: Ensuring desired levels of protection for Federal systems, data, and related assets are achieved (e.g., identification/authentication, access control, encryption, intrusion detection, verification, digital signature, user management, role/privilege management, audit trail capture/analysis).

Collaboration: Communications, messaging, information sharing, scheduling and task management activities (e.g., email, threaded discussions, document library, shared calendaring, task management).

Search: Searching, querying, and retrieving data from multiple sources (e.g., precision/recall ranking, classification, pattern matching)

Communications: Voice, data, and video communications in multiple formats and protocols (e.g., real time chat, instant messaging, audio/video conferencing, event/news management, community management support, computer/telephony integration, voice communications).

Systems Management: All aspects of systems management (e.g., software distribution/license management, configuration/installation, remote systems control, enhancements/service updates, system resource monitoring, helpdesk support/issue tracking).

Forms Management: Creating, managing, and processing online forms to support business operations (e.g., forms creation, modification).

C.4.2.8 DoD IEA Mission Area Support

The Master Contract provides support for the DoD IEA reference models relating DoD's specialized mission, business, and program areas. Though the DoD IEA is an emerging standard, policy and procedures have been formalized for maintaining, evolving, and using the DoD IEA reference models.

The DoIDEA reference models leverage existing DoD standards and reflect the alignment with the FEA. The Master Contract includes IT support services for DoD's Global Information Grid (GIG) architecture, Business, Warfighter, Intelligence, and Enterprise Information Environment (EIE) mission areas.

C.4.3 IT Management Services

IT Management Services provide support for operations and IT resource management requirements across the Federal government. These services encompass support for all strategic planning, management, and control functions integral to IT initiatives. The IT Management Services provide the foundational support to effectively align IT requirements with Federal government business operations.

IT Management Services provide support for all government lines of business, functions, and service components that comprise the FEA PRM and BRM.

IT Management Services shall enable the development and implementation of enhanced governance capabilities, to efficiently and effectively support government agencies' mission requirements and service delivery operations. The services include, but shall not be limited to, support for the following functions.

C.4.3.1 Controls and Oversight

Development and implementation of management controls and systems required by agencies to evaluate, manage, and monitor program performance relative to IT initiatives (e.g., agency, program, and project-level performance plans for IT initiatives; performance measures to support evaluation and reporting requirements for IT initiatives in compliance with FEA/DoD IEA PRM standards, etc.).

C.4.3.2 Risk Management and Mitigation

Identification of risk and preparation of risk management plans for IT projects, initiatives, and ongoing operations. Contingency planning to ensure continuity of IT operations and service recovery during emergency events (e.g., risk assessments to determine contingency planning requirements for IT operating environments; develop/maintain contingency, Continuity of Operations (COOP), and disaster recovery plans for IT components, develop/implement emergency preparedness systems).

C.4.3.3 Regulatory Development

Facilitate the development of IT policies, guidelines and standards to facilitate implementation of Federal laws and regulations. The services include support for development, implementation and maintenance of systems to support agencies' IT regulatory development, compliance, and enforcement activities (e.g., monitoring/ inspection/auditing of IT regulated activities to ensure compliance).

C.4.3.4 Planning and Resource Allocation

Facilitate the planning of IT investments, as well as determine and manage managing overall IT resources to efficiently and effectively support agencies' mission operations. This service area includes, but shall not be limited to support for the following functions:

Budget Formulation/Execution: Facilitate the integration of budgets and plans, at agency and departmental levels, to effectively link IT functions, activities, and resources with mission objectives.

Capital Planning: Facilitate the selection, management, and evaluation of IT investments relative to Federal government agencies' overall capital asset portfolios.

Enterprise Architecture (EA): Development and use of EA work products to manage current and future needs of Federal government business operations (i.e., "baseline" and "target" architectures). The services include transition planning and migration support for all EA components (e.g., business, information, application, and technology architectures), to advance the development and implementation of "core EA capabilities." The services shall provide support relative to Federal government mandates for measuring and reporting on the completion and usage of EA programs, as well as evaluating results for E-Gov alignment and implementation of Federal lines of business and other cross-governmental initiatives (e.g., SmartBUY, IPv6, HSPD-12).

Strategic Planning: Facilitate the effective alignment of IT requirements/ Information Resource Management (IRM) plans with strategic business plans and program initiatives.

Management Improvements: Development and implementation of improved systems and business practices to optimize productivity and service delivery operations (e.g., analysis, and implementation of improvements in the flow of IT work and program processes and tool utilization, including business system analysis, identification of requirements for streamlining, re-engineering, or re-structuring internal systems/business processes for improvement, determination of IT solution alternatives, benchmarking).

C.4.3.5 IT Security

Development and implementation of management, operational, and technical security controls required by agencies to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.4.3.6 System and Network Controls

Facilitate the planning, development, implementation, and management of system and network control mechanisms to support communication and automated needs. Facilitate the planning, organizing, coordinating, and controlling of the arrangement of the elements of protection and monitoring capabilities, and incident recovery actions of the information environment. The process takes configuration orders; status reports; and operational and functional performance requirements as inputs and provides performance capabilities and service and infrastructure controls as outputs.

System and network controls are controlled by environment standards such as policy and operational guidance. The service control requirements enable network controls and operational performance capabilities.

C.4.4 Cloud Computing

The following is an excerpt from the most recent NIST guidance:

Special Publication 800-146, Cloud Computing Synopsis and Recommendations. The full document can be obtained: See *Attachment J-8 Website References.*

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Cloud Essential Characteristics

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of

location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Service Models

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provide. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

All currently emerging and future Cloud Computing as Service offerings, such as "*X" as a Service,* are within the Scope.

C.4.5 Big Data & Big Data Analytics

NIST is currently in working groups concerning this subject and released a preliminary definition during the October 2014 working Group conference. The following is excerpt from that preliminary release.

Big data consists of advanced techniques that harness independent resources for building scalable data systems when the characteristics of the datasets require new architectures for efficient storage, manipulation, and analysis.

Big data is where the data volume, acquisition velocity, or data representation limits the ability to perform effective analysis using traditional approaches or requires the use of significant horizontal scaling (more nodes) for efficient processing.

C.5 ANCILLARY SUPPORT: SERVICES, SUPPLIES AND CONSTRUCTION

The Contractor may provide ancillary support as necessary to offer an integrated IT services-based solution. The ancillary support described here may only be included in a Task Order when it is integral to and necessary for the IT services-based effort. Ancillary support may include, but is not limited to, such things as: clerical support; data entry; subject matter expertise; server racks, mounts, or similar items; and construction, alteration, and repair to real property; and Telecommunications, Wireless, and Satellite services and goods.

(i) The Ordering Contracting Officer (OCO) may allow, and the Contractor may propose, a labor category or labor categories in support of ancillary products and/or support services at the Task Order level not identified in the Standard IT Service Labor Category (LCAT) list, provided that the Contractor complies with all applicable contract clauses and labor laws, including the Service Contract Labor Standards or the Wage Rate Requirements (Construction) and Related Acts, if applicable. *See Section B.7 and B.8 for additional contract requirements.*

(ii) An OCO's inclusion of new labor categories in support of ancillary support services labor categories in a Task Order does not require PCO approval.

C.6 CONTRACT SECURITY REQUIREMENTS

The Contractor shall abide by all contract cybersecurity requirements located in *Sections H.6, H.7, Attachment J-2,* and related federal policy, and other contract security requirements in *Sections H.8 and H.9.* These requirements cover minimum-security standards for select Contractor systems, the handling of Government sensitive data and information technology, Contractor security clearances, and Homeland Security.

C.7 PERFORMANCE WORK STATEMENT (PWS)

C.7.1 Master Contract PWS

The GSA Alliant 2 GWAC is a results-oriented program seeking Outcome-based performance from every Contractor under the Master Contract. It is a standalone Performance-based Acquisition (PBA) requirement independent from Task Order level PBAs that the issuing federal agency might require. The PBA requirements of the Master Contract are designed to ensure that the Contractor is given freedom to determine how to

meet the Government's performance Objectives at the appropriate performance quality levels. This Master Contract PWS includes (1) Contractor Engagement, the most critical PWS, described in Section H.19, J-5.A and (2) Small Business Subcontracting, described in Section G.22.

All measurable performance standards in terms of quality, timeliness, quantity, and the method of assessing Contractor performance against performance standards for the Master Contract are established in Section J's *Attachment J-5 Performance Requirements Summary (PRS).* The PRS listings of Performance Standards indicate the acceptable performance level required by the Government to meet the key Master Contract deliverables. The standards will be measured and structured to permit an assessment of the Contractor's performance whereby the results will also be written into the Contractor Past Performance Assessment Reporting System (CPARS) or another contract performance assessment report. The Government will request the Contractor to develop a *Quality Control Plan*, within the time specified in Section F.7, in response to a Government *Quality Assurance Surveillance Plan* (QASP) that will be developed and implemented by the GSA for the PRS Performance Standards after the Effective Date during the first contract year of the Master Contract.

C.7.1.1 Master Contract PWS and Goals for Contractor Engagement

Critical Performance Requirements for Contractor Engagement are further detailed in Section H.19 Contractor Engagement Requirements based upon *Task Order Participation and Production,* and in *Attachment J-5.A Contractor Engagement Performance-based Evaluation Program*.

The primary goals of Contractor Engagement program are (1) to provide federal agencies with responsibly prepared Contractor Proposals/Quotes in response to each Task Order Request for Proposal/Request for Quote (RFP/RFQ) competitively issued under the Master Contract so to help provide best-value solutions to federal agencies' IT services requirements, and (2) to promote, provide, and ensure that those federal agencies employing the Alliant 2 GWAC are consistently receiving adequate and effective competition in response to their RFPs/RFQs, which ultimately results in achieving these end-goals: (a) economic efficiency/costs savings; (b) innovation of transformational technologies; (c) improvements in the quality of services rendered, and; (d) the opportunity for the Government to acquire performance improvements. Achievement of these primary goals are reached through a combination of two measurable Outcomes: (1) Submitting viable Task Order Proposals (*Participation)* and (2) Winning Task Orders (*Production),* which together help provides best-value IT services solutions to the federal agencies.

C.7.1.2 Master Contract PWS for Small Business Subcontracting

There will be substantial subcontracting opportunities for small business, including veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns. Therefore, meeting Small Business Subcontracting Goals described in *Section*

G.22 is applicable only to Other than Small Business Concerns under the Master Contract. PWS requirements are further detailed in *Attachment J-5.B Small Business Subcontracting Performance-based Evaluation Program.*

C.7.2 Task Order PWS

For Task Orders issued under the Master Contract, it is the requiring federal agency OCO that develops and executes their own PWS and PBA methods independent of the Master Contract PWS and PBA requirements. The OCO may use PBA methods to the maximum extent practicable using the following order of precedence: (1) Firm-Fixed-Price Performance-Based Task Orders (2) Performance-Based Task Orders that are not Firm-Fixed-Priced.

C.8 INNOVATIVE SOLUTIONS

The Contractor should approach agency Task Order requirements with technical proposals offering the most innovative solutions possible leveraging the flexibility provided by FEA encompassed in the scope of this Master Contract. The choice to align scope with FEA allows for a "Greenfield Approach" to the adoption of new technologies and innovative solution approaches in both technology and acquisition as they emerge to meet the rapidly changing and demanding dynamic IT services requirements of the federal Government today and in the future.

The Government strongly encourages the Contractor to also continuously prospect for and establish specialized subcontracting relationships and partnerships, especially with innovative small businesses, to further leverage commercially driven emerging and leading edge technologies in support of providing the needed innovation in solving the federal Government's IT services procurement requirements.

C.9 SERVICES NOT IN SCOPE

The Contractor shall not accept or perform work for a Task Order having the PRIMARY purpose of:

1. An ancillary support service, see Section C.5.
2. A requirement that primarily uses employees not employed in a bona fide executive, administrative, or professional capacity as defined in 29 CFR Part 541 and/or employees primarily employed as labor or mechanics as defined in FAR Subpart 22.401.
3. Inherently Governmental Functions as defined in FAR Subpart 2.101(b).
4. Personal Services as defined in FAR Subpart 2.101(b).
5. Architect & Engineering (A&E) Services as defined in FAR Subpart 2.101(b) and subject to the Brooks Architect-Engineers Act (40 U.S.C. 1102).
6. Armed Guards or,
7. Hazmat Abatement.

C.10 SCOPE REFERENCES AND RESOURCES

The following resources are offered in support of the overall concept and scope of the Master Contract:

- FEA Reference Model: See Attachment J-8 Website References.
- DoD IEA Reference Model: See Attachment J-8 Website References.
- FPDS PSC Manual: See Attachment J-8 Website References.
- DoL BLS SOCs: See Attachment J-8 Website References.
- The Occupational Information Network (O*NET) System (see Attachment J-8 Website References) - is a comprehensive database of occupational competency profiles. The O*NET system is based on the Standard Occupational Classification (SOC) system and also provides information on additional detailed occupations within a SOC category in selected instances.
- Definition of Information Technology (IT)
  - Federal Acquisition Regulations (FAR) Information Technology is defined in FAR Subpart 2.101(b). See Attachment J-8 Website References.
  - Clinger-Cohen Act: See Attachment J-8 Website References.

(END OF SECTION C)